

Chat@Secure LLM

情報コンシェルジュLLM

Azure版



ビジネス仕様の
大規模言語モデル(LLM)
アプリケーション

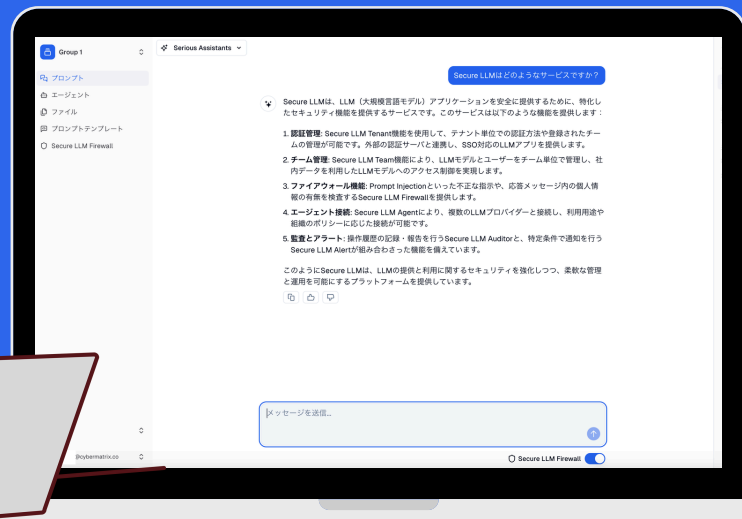


社内の情報の共有できていない。
マニュアルはあるが周知できていない。
社内のいろんな情報が散在している。

カスタマイズしたLLM を
活用して、社内やプロジェクト用の
エージェントを作りたい

しかし、情報漏洩など
セキュリティが不安

情報コンシェルジュLLMは
「Secure LLM」で守られています。



Chat@Secure LLM

情報コンシェルジュLLM

チームのマニュアルや資料などの文書をLLMに学習させ、LLMを社内の情報コンシェルジュとして利用するLLMアプリケーションです。

導入の流れ

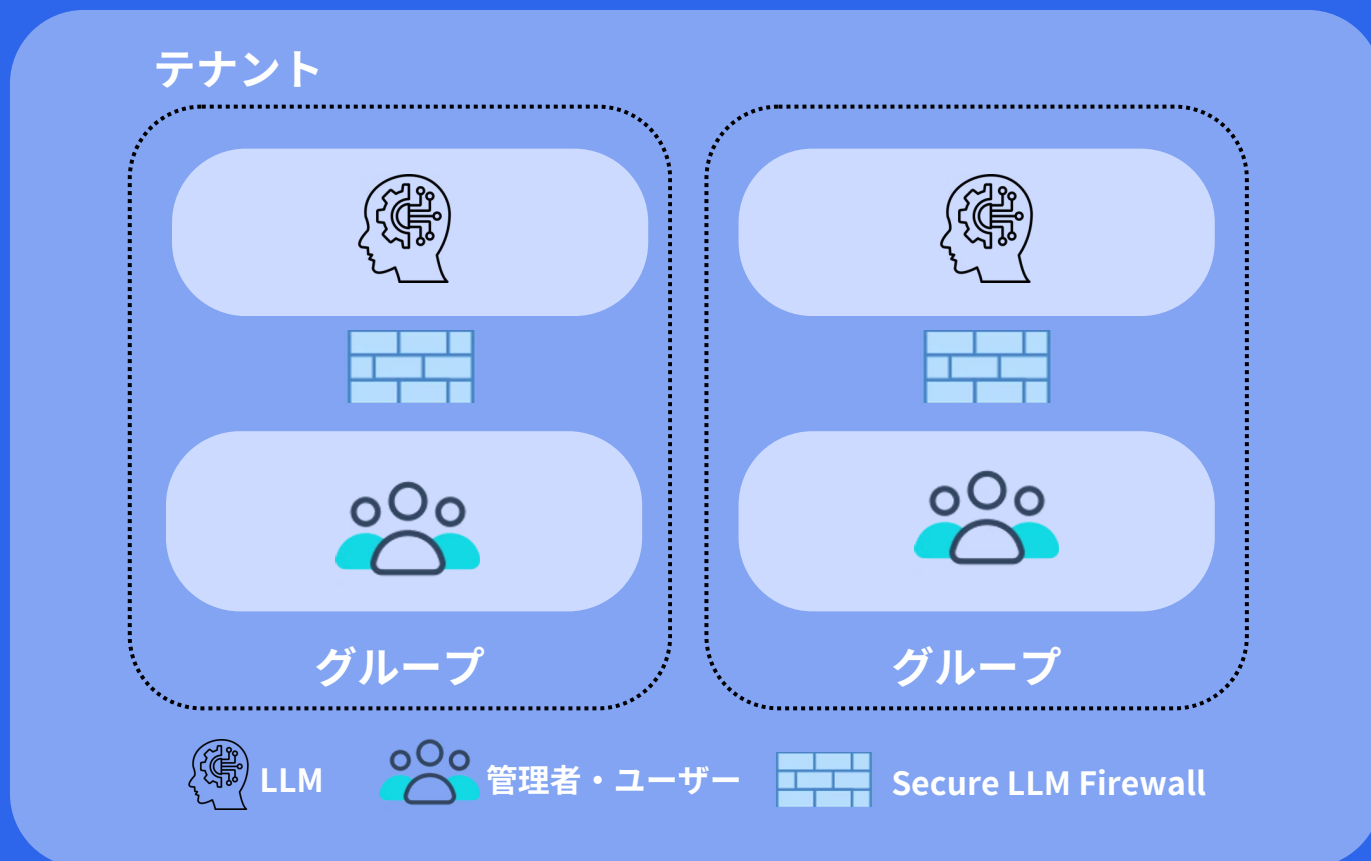
1. テナント管理者によりグループ管理者とグループを作成
2. グループ管理者は文書をアップロードして、情報コンシェルジュ(LLM)を作成
3. 情報コンシェルジュができたなら利用者を作成

Azure版について

Azure版はChat@Secure LLMをAzureのAzure Open AIとAzure EntraIDを利用するサービスです。情報コンシェルジュはお客様が契約したAzureテナント上のOpen AIを利用します。Azure EntraIDは認証を行うため利用します。

サービスを利用するにはお客様のAzureのテナントが必要になります。

Secure LLMのセキュリティ



- ユーザーとLLMをグループ化し、アクセスを制御
- ユーザーから問い合わせ内容をファイアウォールで監視
- ユーザーのアクセス、操作を記録

Secure LLMでは情報のアクセス制御と監視を行うことで情報を統制し、情報コンシェルジュを安全に運用することができます。

サイバー攻撃からビジネスを守ります。

サイバーマトリックス株式会社

Cyber Matrix Co., Ltd.

✉ toiawase@cybermatrix.co

🌐 <https://www.cybermatrix.co>

